

Cisco MultiNet Secure/IP



This chapter provides information on the Cisco MultiNet Secure/IP software product. The information is organized into the following sections:

- Product Overview
- Standard Features
- Product Numbers

Product Overview

Cisco MultiNet Secure/IP protects OpenVMS VAX and Alpha systems from unauthorized user access in a TCP/IP network. MultiNet Secure/IP uses token-based authentication to secure the networked OpenVMS system. Networked systems are most exposed to the risk of break-ins when user passwords are transmitted over the Internet in cleartext. With MultiNet Secure/IP, traditional passwords are replaced with a hand-held or software “token” and a one-time password. One-time passwords, if captured, are useless in the hands of others.

Cisco MultiNet Secure/IP provides a cost-effective, flexible security solution for protecting a user’s OpenVMS systems from the Internet. It supports the leading token vendors on the market, offering a choice of token solutions to meet customers’ security requirements.

Standard Features

Cisco MultiNet Secure/IP software includes the following features:

- Protects networked OpenVMS systems against unauthorized user access

Protects your TCP/IP network by authenticating your remote users at login time, or when accessing the network via FTP or Telnet without exposing their passwords to intruders. Traditional passwords are typically transmitted in cleartext, making them vulnerable to theft and subsequent misuse. With MultiNet Secure/IP, even if the password is captured, it is useless without the corresponding token.



- Secures access from the Internet

Cisco MultiNet Secure/IP is invaluable in wide-area networks, over dial-up lines, and, in particular, on the Internet, where electronic eavesdropping for passwords is prevalent. The growth in distributed client/server and mobile computing means more users are connecting to the enterprise remotely, increasing the risk associated with traditional plaintext passwords crossing the network. MultiNet Secure/IP decreases the risk of your network being compromised in this environment. Network firewalls alone are not enough to safeguard corporations where Internet access is concerned.

- Authenticates remote users at login time or when accessing the network via File Transfer Protocol (FTP) or Telnet

- Uses two-factor authentication

Users are authenticated based on two factors: something secret that the user knows, and something the user possesses. To gain access, a secret Personal Identification Number (PIN) that only users know, is combined with a token that users possess to generate one-time passwords that—alone—are useless if captured since, as the name implies, they are never the same. Cisco MultiNet Secure/IP is the only OpenVMS solution that supports a variety of tokens, including Security Dynamics' SecurID card, Digital Pathway's SecureNet key card, CRYPTOCARD's RB-1 calculator token, and Bellcore's S/KEY soft token.

- Simplifies network security administration

Network administrators can authorize users either individually or in groups. In addition, Cisco MultiNet Secure/IP makes administration of all types of tokens easy by offering one single management utility. MultiNet Secure/IP can be installed as a standalone system or on a cluster-wide basis, further reducing the effort required to make your network more secure.

- Provides seamless integration with OpenVMS

Provides seamless OpenVMS integration by extending the normal OpenVMS login facilities to support token-based authentication. At login time, users are provided with the familiar OpenVMS login environment; existing user or system login procedures do not have to be modified.

- Completes existing security features in Cisco MultiNet for OpenVMS

Cisco MultiNet Secure/IP complements the extensive security features already built into the MultiNet family of TCP/IP products. Cisco MultiNet for OpenVMS includes the Kerberos user authentication technology developed at MIT. Because MultiNet Secure/IP can be configured to use Kerberos passwords, remote users get their Kerberos tickets for trusted logins with a single login through MultiNet Secure/IP.

Token Vendors

Cisco MultiNet Secure/IP supports the following tokens:

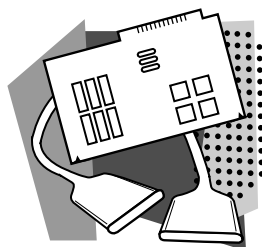
- Security Dynamics SecurID card or PINPAD cards (SD200 and SD520)
- Digital Pathway's SecureNet key (SNK-004 and SNK-010)
- CRYPTOCARD RB-1 calculator token
- Bellcore S/KEY soft token, included with Cisco MultiNet Secure/IP, and the S/KEY software for Windows and Macintosh computers, which is provided free of charge on the MultiNet Secure/IP distribution media

Token vendors can be reached at the following locations:

- Security Dynamics, One Alewife Center, Cambridge, MA 02140-2312, Phone: 617 547-7820, Fax: 617 354-8836
- CRYPTOCARD, Inc., 1649 Barclay Blvd., Buffalo Grove, IL 60089, Phone: 708 459-6500, Fax: 708 459-6500
- Digital Pathways, 201 Ravendale Drive, Mountain View, CA 94043, Phone: 415 964-0707, Fax: 415 961-7487

Prerequisite Software

Cisco MultiNet Secure/IP requires Cisco MultiNet 4.0 for OpenVMS and OpenVMS VAX V6.0 or later, or OpenVMS Alpha V1.5 or later.



Product Numbers

Cisco Secure/IP is included on the MultiNet for OpenVMS media, but is activated by ordering one of the following license key products. Table 301 lists the product numbers you can use to order the licenses. For documentation product numbers, refer to the "Internet Products" section in the "Documentation" chapter, later in this catalog. Cisco Secure/IP is platform independent and runs on both VAX and Alpha OpenVMS platforms.

Table 301 Cisco MultiNet Secure/IP Product Numbers

Description	Product Number
Cisco MultiNet Secure/IP for OpenVMS, 10 users	SIP-VMS-10
Cisco MultiNet Secure/IP for OpenVMS, 20 users	SIP-VMS-20
Cisco MultiNet Secure/IP for OpenVMS, 50 users	SIP-VMS-50
Cisco MultiNet Secure/IP for OpenVMS, 100 users	SIP-VMS-100
Cisco MultiNet Secure/IP for OpenVMS, 250 users	SIP-VMS-250
Cisco MultiNet Secure/IP for OpenVMS, 500 users	SIP-VMS-500
Cisco MultiNet Secure/IP for OpenVMS, 1000 users	SIP-VMS-1000
Cisco MultiNet Secure/IP for OpenVMS, site license	SIP-VMS-SITE

